CLAIMS:

Sub a1

1. An encryption method wherein at least one cryptographic sub-operation is performed on digital data stored as at least one data bit word in a storage cell (10) or a register, characterized in that
a data bit word generated on the basis of random numbers is stored in a storage cell (10) before a data bit word is written therein.

2. An encryption method as claimed in Claim 1,
characterized in that
the bit word based on random numbers is written into the storage cell (10) by a processor.

3. An encryption method as claimed in Claim 1,
characterized in that
the bit word based on random numbers is written into the storage cell (10) via a direct connection between a random number source (12) and the storage cell.

4. An encryption method as claimed in one of the preceding Claims,
characterized in that
the bit word based on random numbers is stored in the storage cell (10) at an instant in time which precedes the cryptographic sub-operation.